

REMARKS

Applicant respectfully requests reconsideration and allowance of the subject application. Claims 1-54 are pending in the application.

Claim Rejections under 35 U.S.C. § 102

Claims 16, 18, 39 and 43-47 stand rejected under 35 U.S.C. § 102 as being anticipated by U.S. Patent Pub. No. 2002/0104019 to Chatani et al. (hereinafter, "Chatani"). Applicant respectfully traverses the rejection.

Independent claim 16 recites a method comprising:

retrieving a console-based key stored on a game console;

retrieving a title-based key associated with a game title running on the game console; and

deriving one or more keys from the console-based key and the title-based key.

Meanwhile, Chatani describes a product distribution and payment system for limited use or otherwise restricted digital software products. A software product, such as a game or video, is made available to customers either through a detachable local storage medium (e.g. a DVD or CD-ROM disc) or over a network connection. The software product is a limited use product in that its use is either restricted to a number of plays or for a limited duration. Chatani also describes a two way, public/private key encryption system that is implemented to transmit the product and usage information between the server that is providing the product and the customer computer system. (*Chatani*, page 1, paragraph 6).

In one example, Chatani describes a method where the server and customer communicate through online means in order to decrypt the software product

1 (Chatani, page 1, paragraph 6), as illustrated by Chatani's Fig. 2B reproduced
2 below. Here, the server computer 222 provides a software product (or "title")
3 requested by the user 220. To ensure secure distribution of the product over the
4 network, the exchange between the server and the user incorporates a multi-
5 layered public key encryption (PKCS) to enable decryption of the software
6 product content stored on the storage media (e.g. DVD), which the user has placed
7 in the console. (Chatani, page 4, paragraph 32).

8 Next, a first pair of keys ("User A" and "User B") 226 is created by the
9 server for facilitation of the decryption process. (Chatani, page 4, paragraphs 32-
10 33). A second pair of keys ("Console A" 228 and Console B" 229) is also
11 created. After certain keys are passed between the server and user (as illustrated
12 in Fig. 2B) in order to develop secure communications, the user transmits the title
13 ID of the software the user wishes to purchase to the server. The server then
14 retrieves title private key ("Title B") 232 for the software product specified by the
15 user, and encrypts and transmits this key to the user. The user then decrypts the
16 software title using the title public key (Title A). (Chatani, page 4, paragraph 33).
17 After decryption, the user transmits purchase information to the server, and the
18 software product will function on user's console for a limited period or for a
19 limited number of uses. (Chatani, page 4, paragraph 34). This process is depicted
20 in Chatani's Fig. 2B:
21
22
23
24
25

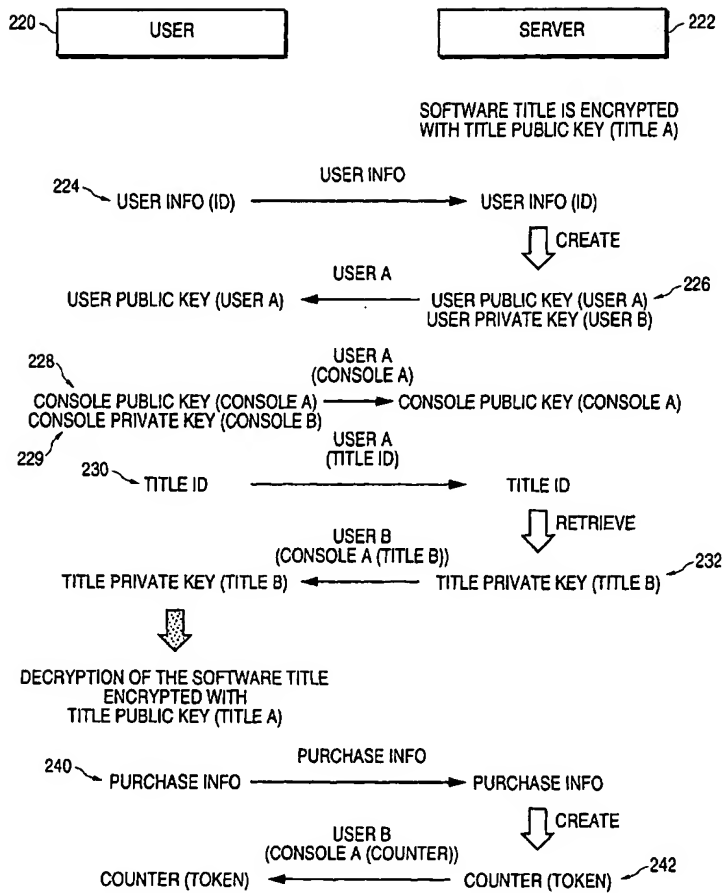


FIG. 2B

Chatani does not disclose “retrieving a title-based key associated with a game title running on the game console,” as required by Applicant’s claim 16. Chatani also fails to disclose “deriving one or more keys from the console-based key and the title-based key,” also required by claim 16.

The Office, however, cites Chatani as disclosing all elements of Applicant’s claim 16. For support, the Office tells Applicant to “see paragraphs 0029, 0033-0036, 0051 [and] Figs. 2B, 3A” of Chatani. (*Office Action of 7/12/05*, page 2).

1 Applicant again respectfully submits, however, that Chatani does not
2 disclose “retrieving a title-based key *associated with a game title running on the*
3 *game console.*” (emphasis added). In Chatani, the only console present is
4 controlled by the user. While the user may have a software product, such as a CD-
5 ROM, in the console, the user does not have permission to play the title until the
6 server gives the user an appropriate key with which to decrypt the product. As
7 discussed above and illustrated in Fig. 2B, part of this method described by
8 Chatani includes the *server* retrieving the title private key (Title B) in response to
9 the user’s request, as Chatani states in the following passage cited by the Office:

10 The user 220
11 next transmits the title ID to the server 222 for the software
12 product to be purchased. The server 222 retrieves title
13 private key (Title B) 232 for the specified software product.

14 . . .

15 The user then decrypts the encrypted
16 software title using the title public key (Title A).

17 (*Chatani*, page 4, paragraph 33). Therefore, as supported by the above
18 passage cited by the Office, the retrieval of the title private key occurs *before* the
19 user is granted access to play the software product located in the game console.
20 Furthermore, Applicant notes that Chatani does not disclose the “retrieval” of any
21 other title key. Therefore, Chatani does not disclose “retrieving a title-based key
22 *associated with a game title running on the game console,*” as required by
23 Applicant’s claim 16. Applicant notes that this is a logical result, as the purpose of
24 Chatani is to use secure communications in order to grant the user access to a
25 specified software product. As the reference does not disclose all of the elements

1 of Applicant's claim, it cannot be said to anticipate. For at least this reason,
2 Applicant respectfully requests that the §102 rejection be withdrawn and claim 16
3 be forwarded onto issuance.

4 Additionally, Applicant respectfully submits that Chatani does not disclose
5 "deriving one or more keys from the console-based key and the title-based key."
6 As illustrated above in Fig. 2B, after the title private key is retrieved by the server
7 and transmitted to the user, the user decrypts the software title. After doing so, the
8 user transmits purchasing information to the server. The server may then
9 correspondingly create a usage counter for determining the amount of uses or the
10 length of time that the user is entitled to use the software title for. (*Chatani*, page
11 4, paragraph 34). Nowhere does Chatani disclose "deriving one or more keys
12 from the console-based key and the title-based key." To the contrary, once the
13 decryption has occurred, no more keys need be derived at all as the purpose of
14 Chatani has already been achieved.

15 Furthermore, if any further communications occur between the server and
16 the user, the original public/private key pair ("User A" and "User B") is used, or a
17 new public/private key pair is created. (*Chatani*, page 4, paragraph 35). This also
18 supports the conclusion that neither the later-created console key pair ("Console
19 A" and "Console B"), nor the title key pair ("Title A" and "Title B") are used for
20 "deriving one or more keys."

21 As Chatani does not disclose this feature, it cannot be said to anticipate.
22 For at least this additional reason, Applicant respectfully requests that the §102
23 rejection be withdrawn and claim 16 be forwarded onto issuance.
24
25

1 **Dependent claim 18** depends from claim 16 and is allowable by virtue of
2 this dependency. Moreover, this claims recites features that, when taken together
3 with those of claim 16, define a method not disclosed by Chatani.

4 **Independent claim 39** recites a computer-readable medium for a game
5 console comprising computer-executable instructions that, when executed, direct
6 the game console to:

7 obtain a first key stored in memory of the game console and a
8 second key associated with a game title running on the game console; and

9 derive one or more keys from the first and second keys.

10
11 For the reasons given above with respect to claim 16, Chatani does not
12 disclose this device. Namely, the cited reference does not disclose obtaining a
13 “second key associated with a game title running on the game console,” nor does it
14 disclose deriving “one or more keys from the first and second keys.”

15 Applicant therefore respectfully requests allowance of claim 39 for at least
16 the same reasons described above with respect to claim 16.

17 **Independent claim 43** recites a game console, comprising:

18 a memory to store a first key;

19 a game title configured to execute on the game console, the game
20 title having an associated second key; and

21 a processor coupled to the memory, the processor being configured
22 to derive at least one cryptographic keys from the first and second keys.

23 For the reasons given above with respect to claim 16, Chatani does not
24 disclose this device. Namely, the cited reference does not disclose “a processor
25

1 coupled to the memory, the processor being configured to derive at least one
2 cryptographic keys from the first and second keys.” Again, when the title private
3 key has been retrieved and the software decrypted by the user, there is no need for
4 the Chatani method to derive any more keys.

5 Applicant therefore respectfully requests allowance of claim 43 for at least
6 the same reasons described above with respect to claim 16.

7 **Dependent claims 44-47** depend from claim 43 and are allowable by virtue
8 of this dependency. Moreover, these claims recite features that, when taken
9 together with those of claim 43, define game consoles not disclosed by Chatani.

10 For Example, **dependent claim 44** recites “a game console as recited in
11 claim 43, wherein the memory comprises a read only memory.” Also, **dependent**
12 **claim 45** recites “a game console as recited in claim 43, wherein the processor is
13 configured to compute a hash function of the first and second keys.”

14 However, in making out a rejection of claims 44 and 45, the Office merely
15 made the following statement:

16 Regarding claims 43-45, Chatani et al. disclose a memory to store a first key (see
17 paragraphs 0016, 0024, 0032), a game title configured to execute on the game console, having an
18 associated second key (see paragraph 0029), and a processor coupled to the memory, configured
19 to derive at least one cryptographic key from the first and second key (see paragraphs 0016,
20 0032-0036; figures 2B, 3A).

21 (*Office Action of 7/12/05*, page 2). Applicant respectfully submits that the
22 Office has not indicated anywhere in this analysis where Chatani discloses the
23 added features of claims 44 and 45. As Chatani has not been shown to disclose all
24 of the elements of Applicant’s claims, Applicant respectfully requests that the §102
25

1 rejections be withdrawn. Claims 44 and 45 are allowable for at least this
2 additional reason.

3
4 **Claim Rejections under 35 U.S.C. § 103**

5 Claims 1, 4-6, 8-13, 15, 19-26 and 48-51 stand rejected under 35 U.S.C. §
6 103(a) as being unpatentable over U.S. Patent No. 6,152,824 to Rothschild et al.
7 (hereinafter, "Rothschild") in view of U.S. Patent No. 5,586,257 to Perlman.

8 Claim 17 stands rejected under 35 U.S.C. § 103(a) as being unpatentable
9 over Chatani in view of U.S. Patent No. 6,006,266 to Murphy Jr. et al. (hereinafter
10 "Murphy").

11 Claims 2, 3, 7, 14, 27, 30-38, 49 and 52-54 stand rejected under 35 U.S.C. §
12 103(a) as being unpatentable over Rothschild in view of Perlman in further view
13 of Chatani.

14 Claims 40-42 stand rejected under 35 U.S.C. § 103(a) as being unpatentable
15 over Rothschild in view of Perlman in further view of U.S Patent Pub. No.
16 2002/0071557 to Nguyen.

17 Claim 28 stands rejected under 35 U.S.C. § 103(a) as being unpatentable
18 over Rothschild in view of Perlman and Chatani in further view of Murphy.

19 Claim 29 stands rejected under 35 U.S.C. § 103(a) as being unpatentable
20 over Rothschild in view of Perlman and Chatani in further view of Nguyen.

21 Applicant respectfully traverses these rejections.
22
23
24
25

1 Rothschild in view of Perlman

2 Claims 1, 4-6, 8-13, 15, 19-26 and 48-51 stand rejected under 35 U.S.C. §
3 103(a) as being unpatentable over Rothschild in view of Perlman. Applicant
4 respectfully traverses the rejection.

5 **Independent claim 1** recites a method comprising:

6 deriving a secret that is unique to a game console running a
7 particular game title; and

8 establishing a secure communication link between multiple
9 game consoles over a local area network using the secret.

10 In making out a rejection of claim 1, the Office states that Rothschild
11 discloses all of the elements of Applicant's claim, except for the "local area
12 network." The Office, however, cites Perlman for this element, and states that "it
13 was well known in the art at the time of the invention that multiple gaming
14 consoles that communicate over a network such as the internet can communicate
15 equally as well over a local are network." (*Office Action of July 12, 2005*, pages
16 3-4).

17 Rothschild describes an online gaming system and process arranged in a
18 client/server online gaming architecture. In Rothschild, the client computers are
19 configured to run a client gaming program, and the server computers are coupled
20 to the client computers via a network. The server computers run multiple server
21 programs, including a master control program ("MCP") that governs access of the
22 server programs to the online gaming architecture. Server computers also run a
23 matchmaker program ("MM") that supports rendezvous services for connecting
24 players. (*Rothschild*, abstract).
25

1 Perlman describes a system for linking a first computer to a second
2 computer. The system also includes a server that is coupled to the network for
3 receiving a request for direct linking from both computers. The two computers are
4 then matched via matching criteria and a communication link between the
5 computers is established. (*Perlman*, abstract).

6 Neither reference discloses “deriving a secret that is unique to a game
7 console running a particular game title” as recited in Applicant’s claim 1.

8 For support that Rothschild discloses such an element, the Office directs
9 Applicant’s attention to the following passage:

10 2

11 In one embodiment, a networked computer on-line gam-
12 ing system is arranged in a client/server online gaming
13 architecture and utilized to run gaming programs. The Client
14 computers are configured to run a gaming Client program.
15 5 The Server computers are coupled to the Client computers
16 via a network. The Server computers run Server programs
17 including a Master Control Program (MCP) that governs
18 access of the server programs to the online gaming
19 architecture, a Servorum program (SV) for creating
20 10 instances of a server program, a Matchmaker program (MM)
21 that supports rendezvous services, a Game Instances Class
22 Server program (GICS) that enables features of the online
23 gaming architecture to be Utilized, and Game Upper Level
24 Protocol server program (GULP) associated with said GICS.
25 15

20 (*Rothschild*, Col. 2, lines 1-14). This passage, however, only describes the
21 server/client relationship discussed above, and in particular discusses how a server
22 program runs an MCP in order to govern access to the online gaming architecture.
23 This passage does not mention how the MCP governs such access, nor what is
24 involved for a client computer to gain such access. Applicant therefore
25 respectfully submits that the above passage does not mention, nor teach or suggest,

1 “deriving a secret that is unique to a game console running a particular game title.”

2 If the Examiner intends to maintain the rejection, Applicant requests that the
3 Examiner distinctly point out how Rothschild teaches such a claim.

4 Because not all of the elements of Applicant’s claim 1 have been addressed,
5 Applicant respectfully submits that the Office has not presented a *prima facie* case
6 of obviousness. As such, the § 103 rejection should be withdrawn and claim 1
7 should be forwarded onto issuance.

8 **Dependent claims 4 and 5** depend from claim 1 and are allowable by
9 virtue of this dependency. Moreover, these claims recite features that, when taken
10 together with those of claim 1, define methods not taught or suggested by
11 Rothschild and Perlman.

12 **Independent claim 6** recites a method comprising:

13 generating at least one key that is secret to an authentic
14 gaming system running an authentic game title;

15 discovering whether another gaming system on a common
16 local area network is hosting the game title; and

17 establishing a secure communication link between multiple
18 gaming systems to facilitate multi-system play of the game title over
the local area network.

19 In making out a rejection of claim 6, the Office cites Rothschild as teaching
20 the “discovering” element of Applicant’s claim. (*Office Action of 7/12/05*, page
21 4). This cited portion of Rothschild, however, teaches a client computer program
22 (or “gizmo”) discovering the net address of a server MCP and attempting to attach
23 to the MCP. (*Rothschild*, col. 4, lines 6-18). Rothschild defines server computers
24 earlier in the specification. According to Rothschild, “[s]ervers are typically
25

1 computers which are not attended by any person but which are accessible via the
2 net for the interchange of data messages to and from any client.” (*Rothschild*, col.
3 3, lines 58-61). As such, Rothschild does not teach or suggest a “gaming system .
4 . . hosting the game title,” but rather teaches a client computer program connecting
5 to an unmanned server. A client computer program attempting to access a server
6 MCP does not constitute “discovering whether another *gaming system* on a
7 common local area network is hosting the game title,” as an unmanned server is
8 not a gaming system. As neither Rothschild nor Perlman teach this element of
9 Applicant’s claim, the § 103 rejection should be withdrawn and claim 1 should be
10 forwarded onto issuance.

11 Similarly, the Office cites Rothschild as teaching the “establishing” portion
12 of Applicant’s claim. The portion of Rothschild cited by the Office describes a
13 client computer program authenticating itself with an MCP before the client
14 computer program is able to use any of the services provided by the MCP. Again,
15 this authentication process involves a private key exchange via a first public key
16 exchange. After the key exchange, a secure link between the client computer
17 program and the server MCP can be established. (*Rothschild*, col. 4, line 51- col.
18 5, line 24).

19 Again, however, an MCP is a program being run by an unmanned server,
20 and not by a “gaming system.” Therefore, the cited passage of Rothschild does
21 not teach “establishing a secure communication link *between multiple gaming*
22 *systems* to facilitate multi-system play of the game title over the local area
23 network.” (emphasis added). Instead, it teaches establishing a connection
24 between a client computer program and an *unmanned server*. For at least this
25

1 additional reason, the § 103 rejection should be withdrawn and claim 6 should be
2 forwarded onto issuance.

3 **Dependent claims 8-12** depend from claim 6 and are allowable by virtue of
4 this dependency. Moreover, these claims recite features that, when taken together
5 with those of claim 6, define methods not taught or suggested by Rothschild and
6 Perlman.

7 **Independent claim 13** recites a method comprising:

8
9 broadcasting, from a client game console over a local area
10 network, a request to join in playing a game title in a network
11 gaming session being hosted by a host game console, the request
12 containing a secret that is unique to the client game console running
13 the game title; and

14
15 broadcasting, from the host game console over the local area
16 network, a reply to the request, the reply containing information that
17 can be used to establish a secure communication link.

18
19 For the reasons given above with respect to claims 1 and 6, Rothschild and
20 Perlman do not teach or suggest this method. Namely, Rothschild and Perlman do
21 not teach or suggest “broadcasting, from a client game console over a local area
22 network, a request to join in playing a game title in a network gaming session
23 being hosted by a host game console.” Instead, Rothschild again teaches a client
24 computer program attempting to connect to an unmanned server MCP. An
25 unmanned server is not a game console, as discussed above in regards to claim 6,
and therefore does not teach or suggest this element of Applicant’s claim.
Furthermore, neither Rothschild nor Perlman teach or suggest “the request

1 containing a secret that is unique to the client game console running the game
2 title” for at least the same reasons as discussed in regards to claim 1.

3 In rejecting claim 13, however, the Office cites a portion of Rothschild that
4 is not cited in the rejection of claim 1, and therefore the rejection merits additional
5 discussion. Applicant respectfully submits that the additional portion of
6 Rothschild, nor Rothschild in its entirety, teaches or suggests Applicant’s claim 13.
7 In particular, the reference does not teach “a secret that is unique to the client
8 game console running the game title.” Again, Rothschild teaches a client
9 computer program attaching to an MCP, and authenticating itself with the MCP via
10 a public/private key exchange. If the client computer program has never
11 previously authenticated itself with the MCP, then the client must “obtain a private
12 key (PK) for the strong private key encryption method supported by that particular
13 MCP.” (*Rothschild*, col. 4, lines 4-59). Nowhere, however, does Rothschild teach
14 or suggest using a “secret that is *unique to the client game console*,” as recited in
15 Applicant’s claim 13. (emphasis added). Instead, in Rothschild, the client
16 computer program *requests* a key from the server MCP, a key that is not unique to
17 the client computer program but rather is a PK that is “supported by that particular
18 MCP.” Therefore, the key is not related at all to the client game console. If
19 anything, the key is related to the server MCP and not the client, and thus is
20 exactly opposite of the element recited in Applicant’s claim. As such, Rothschild
21 teaches away from claim 13. For at least this additional reason, Applicant
22 respectfully requests allowance of claim 13.

23 **Dependent claim 15** depends from claim 13 and is allowable by virtue of
24 this dependency. Moreover, this claim recites features that, when taken together
25

1 with those of claim 13, define a method not taught or suggested by Rothschild and
2 Perlman.

3 **Independent claim 19** recites a method comprising:

4 creating a request to join in playing a game title being hosted
5 by a host game console on the local area network;

6 broadcasting the request over the local area network;

7 receiving a reply from the host game console, the reply
8 containing one or more session keys; and

9 using the session keys from the reply to facilitate future
10 secure communication with the host game console.

11 For the reasons given above with respect to claims 6 and 13, Rothschild and
12 Perlman do not teach or suggest this method. Namely, Rothschild and Perlman do
13 not teach or suggest “creating a request to join in playing a game title being hosted
14 by a host game console,” as a server MCP does not constitute a host game console.

15 Applicant therefore respectfully requests allowance of claim 19.

16 **Dependent claims 21-24** depend from claim 19 and are allowable by virtue
17 of this dependency. Moreover, these claims recite features that, when taken
18 together with those of claim 19, define methods not taught or suggested by
19 Rothschild and Perlman.

20 **Independent claim 25** recites a method comprising:

21 forming an initial packet that contains first data used to derive
22 a cryptographic key;

23 computing a first hash digest of the initial packet;
24
25

1 sending the initial packet and the first hash digest to another
2 game console on the local area network that is playing the same
3 game title;

4 receiving a reply packet from the other game console, the
5 reply packet including a second hash digest and second data;

6 authenticating the reply packet using the second hash digest;
7 and

8 deriving one or more security association keys from the first
9 and second data, the security association keys being used to secure
10 communication between the multiple consoles.

11 For the reasons given above with respect to claims 6 and 13, Rothschild and
12 Perlman do not teach or suggest this method. Namely, Rothschild and Perlman do
13 not teach or suggest "multiple consoles." For at least this reason, Applicant
14 respectfully requests allowance of claim 25.

15 Furthermore, Rothschild and Perlman do not teach or suggest "computing a
16 first hash digest," as recited in claim 25. For teaching such an element, the Office
17 cites the following passage of Rothschild:

18 If the Gizmo already has a PK (for that particular MCP)
19 that was obtained during some previous authentication, then,
20 referring to FIG. 7, the Gizmo attempts to use that PK for
21 authentication (steps 40, 41, 42, 43, 44, 45) and if successful
22 (step 46) it uses a new PK obtained from the MCP (in step
23 45) for use during the present session. If this attempt fails (a
24 likely reason being that PK is either stale or forgotten by the
25 said MCP) then the Gizmo falls back upon public key
cryptographic exchange with the MCP to obtain a new PK
(steps 47, 48). As previously suggested a public key cryp-
tographic exchange (steps 47, 48) is more computationally
intense and so takes much longer than a strong private
encryption key exchange using a PK. The same PK is used
for encryption/decryption for traffic passing both ways, so
long as the PK remains in effect. As a result of the steps 40
through 48, the Gizmo and MCP have a secure mutual link
(steps 49, 50).

1 (Rothschild, col. 5, lines 8-24). Applicant respectfully submits, however,
2 the that the preceding passage merely teaches the how the client computer
3 program accesses a server MCP. According to the passage, the client may be able
4 to use a previously-obtained PK if the client has previously accessed the MCP, and
5 if the MCP remembers the client and the client's PK. Otherwise, the client may
6 need to go through the entire public/private key exchange again, as discussed
7 above. The passage does not, however, mention the term "hash," nor suggest that
8 one may "compute a hash digest of an initial packet." As such, Rothschild and
9 Perlman have not been shown to teach all of the elements of Applicant's claim 25.
10 For at least this additional reason, Applicant respectfully requests allowance of
11 claim 25.

12 **Dependent claim 26** depends from claim 25 and is allowable by virtue of
13 this dependency. Moreover, this claim recites features that, when taken together
14 with those of claim 25, define a method not taught or suggested by Rothschild and
15 Perlman.

16 **Independent claim 48** recites a game console, comprising:

17 a memory; and

18 a processor coupled to the memory and configured to
19 generate at least one key that is secret to the game console when
20 running an authentic game title, the processor being further
21 configured to discover, using the key, a host game console on a
22 common local area network that is hosting the game title and to
23 establish a secure communication link with the host game console
24 over the local area network.

24 For the reasons given above with respect to claims 6 and 13, Rothschild and
25 Perlman do not teach or suggest this method. Namely, Rothschild and Perlman do

1 not teach or suggest “at least one key that is secret to the game console when
2 running an authentic game title,” nor do they teach both “a game console” and a
3 “host game console.”

4 Applicant therefore respectfully requests allowance of claim 48.

5 **Dependent claims 50-51** depend from claim 48 and are allowable by virtue
6 of this dependency. Moreover, these claims recite features that, when taken
7 together with those of claim 48, define game consoles not taught or suggested by
8 Rothschild and Perlman.

9
10 Chatani in view of Murphy

11 Claim 17 stands rejected under 35 U.S.C. § 103(a) as being unpatentable
12 over Chatani in view of Murphy. In making out a rejection of claim 17, the Office
13 states that the rejection of base claim 16 has been shown to be anticipated by
14 Chatani, and that Murphy teaches the additional element present in claim 17.
15 (*Office Action of 7/12/05*, page 9). Applicant respectfully traverses the rejection.

16 As discussed above, Chatani describes a product distribution and payment
17 system for limited use or otherwise restricted digital software products. (*Chatani*,
18 page 1, paragraph 6). Murphy, meanwhile, describes a system of multiplexing
19 clients and applications among multiple servers. One server is a master server
20 owning a well-known port, and the other servers are slave servers supporting
21 established web browser-to-application state sessions. (*Murphy*, abstract).

22 **Dependent claim 17** recites “a method as recited in claim 16, wherein the
23 deriving comprises computing a hashing function on a concatenation of the
24 console-based key and the title-based key.” As discussed above, **independent**

1 **claim 16** recites a method comprising “retrieving a title-based key associated with
2 a game title running on the game console.”

3 Neither Chatani nor Murphy teach or suggest such an element. In Chatani,
4 the purpose of the key exchange is to allow the user to decrypt the software that
5 may be on the user’s computer or console. Therefore, there is no need to
6 “retriev[e] a title-based key associated with a game title running on the game
7 console.” This is because when the game title is running, the purpose of Chatani
8 has been completed, and there is no longer a need for a user to receive any sort of
9 key. Thus, Chatani effectively teaches away from the claimed element.
10 Furthermore, Murphy is not cited by the Office as teaching such an element, and
11 does not add anything of substance to the rejection. Therefore, for at least the
12 reasons given above with respect to claim 16, Chatani and Murphy do not teach or
13 suggest claim 17.

14 Moreover, claim 17 recites features that, when taken together with those of
15 claim 16, define a method not taught or suggested by Chatani and Murphy.
16 Applicant therefore respectfully requests allowance of claim 17.

17
18 Rothschild in view of Perlman in further view of Chatani

19 Claims 2, 3, 7, 14, 27, 30-38, 49 and 52-54 stand rejected under 35 U.S.C. §
20 103(a) as being unpatentable over Rothschild in view of Perlman in further view
21 of Chatani. Applicant respectfully traverses the rejections.

22 **Dependent claim 2** recites a “method as recited in claim 1, wherein the
23 deriving comprises deriving the secret from data stored in the game console and
24 data associated with the particular game title.” **Dependent claim 3** recites a
25 “method as recited in claim 1, wherein the deriving comprises retrieving a

1 console-based key from the game console and a title-based key associated with the
2 particular game title; and deriving the secret from the console-based key and the
3 title-based key.”

4 In making out a rejection of claims 2 and 3, the Office relies upon the
5 earlier rejection of base claim 1, where the Office rejected the claim as
6 unpatentable over Rothschild in view of Perlman. The Office then cites Chatani as
7 teaching the additional elements of dependent claims 2 and 3. (*Office Action of*
8 *7/12/05*, page 10).

9 As shown above, Applicant respectfully submits that Rothschild and
10 Perlman do not teach or suggest independent claim 1. Namely, the references do
11 not teach “deriving a secret that is unique to a game console running a particular
12 game title.” As Chatani does not teach or suggest such an element, nor is it cited
13 for doing so, the reference does not add anything of substance to the rejection of
14 the base claim. Therefore, dependent claims 2 and 3 are allowable by virtue of
15 this dependency.

16 Moreover, these claims recite features that, when taken together with those
17 of claim 1, define methods not taught or suggested by Rothschild, Perlman and
18 Chatani. The Examiner cites Chatani as teaching the additional elements of claims
19 2 and 3, as listed above. Applicant, however, respectfully submits that Chatani
20 does not disclose “deriving the secret from data stored in the game console and
21 data associated with the particular game title,” as recited in Applicant’s claim 2,
22 nor “deriving the secret from the console-based key and the title-based key,” as
23 recited in Applicant’s claim 3.

24 As illustrated above in Fig. 2B of Chatani, after the title private key is
25 retrieved by the server and transmitted to the user, the user decrypts the software

1 title. After doing so, the user transmits purchasing information to the server. The
2 server may then correspondingly create a usage counter for determining the
3 amount of uses or the length of time that the user is entitled to use the software
4 title for. (*Chatani*, page 4, paragraph 34). Nowhere does Chatani disclose
5 “deriving the secret” from the title private key. To the contrary, once the
6 decryption has occurred, no more keys need be derived at all as the purpose of
7 Chatani has already been achieved.

8 Furthermore, if any further communications occur between the server and
9 the user, the original public/private key pair (“User A” and “User B”) is used, or a
10 new public/private key pair is created. (*Chatani*, page 4, paragraph 35). This also
11 supports the conclusion that neither the later-created console key pair (“Console
12 A” and “Console B”), nor the title key pair (“Title A” and “Title B”) are used for
13 “deriving one or more keys.”

14 For at least this additional reason, claims 2 and 3 are allowable.

15 **Dependent claim 7** recites a “method as recited in claim 6, wherein the
16 generating comprises retrieving a console-based key from the gaming system and
17 a title-based key associated with the game title; and deriving the key from the
18 console-based key and the title-based key.”

19 In making out a rejection of claim 7, the Office relies upon the earlier
20 rejection of base claim 6, where the Office rejected the claim as unpatentable over
21 Rothschild in view of Perlman. The Office then cites Chatani as teaching the
22 additional elements of dependent claim 7. (*Office Action of 7/12/05*, page 10).

23 As shown above, Applicant respectfully submits that Rothschild and
24 Perlman do not teach or suggest independent claim 6. Namely, the references do
25 not teach “discovering whether another gaming system on a common local area

1 network is hosting the game title,” nor “establishing a secure communication link
2 between multiple gaming systems to facilitate multi-system play of the game title
3 over the local area network.”

4 As Chatani does not teach or suggest such an element, nor is it cited for
5 doing so, the reference does not add anything of substance to the rejection of the
6 base claim. Therefore, dependent claim 7 is allowable by virtue of this
7 dependency. Moreover, this claim recites features that, when taken together with
8 those of claim 6, define a method not taught or suggested by Rothschild, Perlman
9 and Chatani.

10 For example, claim 7 is also allowable for the same reasons as discussed
11 above in regards to claims 2 and 3. Namely, Chatani does not teach “deriving the
12 key from the console-based key and the title-based key.” For at least this
13 additional reason, claim 7 is allowable.

14 **Dependent claim 14** recites a “method as recited in claim 13, further
15 comprising deriving the secret from data stored in the client game console and
16 data associated with the game title.”

17 In making out a rejection of claim 14, the Office relies upon the earlier
18 rejection of base claim 13, where the Office rejected the claim as unpatentable
19 over Rothschild in view of Perlman. The Office then cites Chatani as teaching the
20 additional elements of dependent claim 14. (*Office Action of 7/12/05*, page 10).

21 As shown above, Applicant respectfully submits that Rothschild and
22 Perlman do not teach or suggest independent claim 13. Namely, the references do
23 not teach “broadcasting, from a client game console over a local area network, a
24 request to join in playing a game title in a network gaming session being hosted by
25

1 a host game console,” nor “a secret that is unique to the client game console
2 running the game title.”

3 As Chatani does not teach or suggest such an element, nor is it cited for
4 doing so, the reference does not add anything of substance to the rejection of the
5 base claim. Therefore, dependent claim 14 is allowable by virtue of this
6 dependency. Moreover, this claim recites features that, when taken together with
7 those of claim 13, define a method not taught or suggested by Rothschild, Perlman
8 and Chatani.

9 For example, claim 14 is also allowable for the same reasons as discussed
10 above in regards to claims 2 and 3. Namely, Chatani does not teach “deriving the
11 secret from data stored in the client game console and data associated with the
12 game title.” For at least this additional reason, Applicant respectfully requests
13 allowance of claim 14.

14 **Independent claim 27** recites a method comprising:

15
16 retrieving a console-based key from a first game console and
17 a title-based key associated with a game title running on the first
game console;

18 deriving at least one cryptographic key from the console-
19 based key and the title-based key;

20 creating, at a first console, a request to join in playing the
21 game title being hosted by a second game console on the local area
network;

22 cryptographically encoding the request using the
23 cryptographic key;

24 broadcasting the request over the local area network;
25

1 cryptographically decoding the request, at the second game
2 console, using the cryptographic key;

3 generating, at the second game console, a reply that contains
4 at least one session key;

5 cryptographically encoding the reply using the cryptographic
6 key;

7 broadcasting the reply over the local area network;

8 cryptographically decoding the reply, at the first game
9 console, using the cryptographic key;

10 exchanging packets between the first and second game
11 consoles, the packets being protected using the session key and
12 containing data used to derive at least one security association key;
13 and

14 establishing a secure communication link between the first
15 and second game consoles using the security association keys to
16 facilitate secure multi-console play of the game title.

17 In making out a rejection of claim 27, the Office cites Rothschild for many
18 of the elements, but states that Rothschild does “not disclose keys for both the
19 gaming system and the title, and deriving the key from the two.” Nevertheless, the
20 Office cites Chatani as teaching such an element. (*Office Action of 7/12/05*, page
21 11). Applicant respectfully traverses the rejection.

22 For the reasons given above with respect to claims 6 and 13, Rothschild,
23 Perlman and Chatani do not teach or suggest this method. Namely, they do not
24 teach or suggest “exchanging packets between the first and second game
25 consoles,” nor “establishing a secure communication link between the first and
second game consoles,” as a server MCP does not constitute a host game console.

1 Furthermore, Chatani is not cited for teaching such an element, nor does it teach
2 such an element, and therefore does not add anything of substance to the rejection.

3 Furthermore, Chatani does not teach “deriving at least one cryptographic
4 key from the console-based key and the title-based key,” as submitted by the
5 Office. Therefore, claim 27 is additionally allowable for at least the reasons
6 discussed above in regards to claims 2 and 3.

7 Applicant therefore respectfully requests allowance of claim 27.

8 **Dependent claim 32** depends from claim 27 and is allowable by virtue of
9 this dependency. Moreover, this claim recites features that, when taken together
10 with those of claim 27, define an apparatus not taught or suggested by Rothschild,
11 Perlman and Chatani.

12 **Dependent claim 30** recites a “method as recited in claim 27, wherein the
13 exchanging comprises . . . computing a hash digest of the packet.” In making out
14 a rejection of claim 30, the Office relies upon the rejection of base claim 27 and
15 Rothschild for teaching the additional elements of claim 30.

16 As shown above, however, Rothschild, Perlman and Chatani do not
17 disclose independent claim 27. Claim 30, therefore, is allowable by virtue of this
18 dependency. Furthermore, Applicant respectfully submits that Rothschild does
19 not teach “computing a hash digest of the packet,” as discussed above in regards to
20 claim 25. Therefore, claim 30 is additionally allowable for at least the same
21 reasons given above with respect to claim 25.

22 Applicant therefore respectfully requests allowance of claim 30.

23 **Independent claim 33** recites a method comprising:
24
25

1 retrieving a console-based key from a first game console and
2 a title-based key associated with a game title running on the first
3 game console;

4 deriving at least one cryptographic key from the console-
5 based key and the title-based key;

6 creating a request to join in playing the game title being
7 hosted by another game console on the local area network;

8 encoding the request using the cryptographic key;

9 broadcasting the request over the local area network;

10 receiving a reply from a host game console, the reply
11 containing at least one session key;

12 exchanging packets with the host game console, the packets
13 being protected using the session key and containing data used to
14 derive at least one security association key; and

15 establishing a secure communication link with the host game
16 console using the security association key.

17 In making out a rejection of claim 33, the Office cites Rothschild for many
18 of the elements, but states that Rothschild does “not disclose keys for both the
19 gaming system and the title, and deriving the key from the two.” Nevertheless, the
20 Office cites Chatani as teaching such an element. (*Office Action of 7/12/05*, page
21 13). Applicant respectfully traverses the rejection.

22 For the reasons given above with respect to claims 6 and 13, Rothschild,
23 Perlman and Chatani do not teach or suggest this method. Namely, they do not
24 teach or suggest “exchanging packets with the host game console,” nor
25 “establishing a secure communication link with the host game console,” as a
server MCP does not constitute a host game console. Furthermore, Chatani is not

1 cited for teaching such an element, nor does it teach such an element, and
2 therefore does not add anything of substance to the rejection.

3 Furthermore, Chatani does not teach “deriving at least one cryptographic
4 key from the console-based key and the title-based key,” as submitted by the
5 Office. Therefore, claim 33 is additionally allowable for at least the reasons
6 discussed above in regards to claims 2 and 3.

7 Applicant therefore respectfully requests allowance of claim 33.

8 **Dependent claims 34-38** depend from claim 33 and are allowable by virtue
9 of this dependency. Moreover, these claims recite features that, when taken
10 together with those of claim 33, define methods not taught or suggested by
11 Rothschild, Perlman and Chatani.

12 **Dependent claim 49** recites a “game console as recited in claim 48,
13 wherein the processor is configured to derive the key from data stored in the
14 memory and data associated with the authentic game title.” In making out a
15 rejection of claim 49, the Office relies upon the rejection of base claim 48 and
16 Chatani for teaching the additional elements of claim 49.

17 As shown above, however, Rothschild and Perlman do not disclose
18 independent claim 48, nor does Chatani add anything of substance to the rejection
19 of the base claim. Claim 48, therefore, is allowable by virtue of this dependency.
20 Furthermore, Applicant respectfully submits that Chatani does not teach
21 “deriv[ing] the key from data stored in the memory and data associated with the
22 authentic game title,” as discussed above in regards to claims 2 and 3. Therefore,
23 claim 49 is allowable for at least this additional reason.
24
25

1 **Independent claim 52** recites a system, comprising:

2 first and second game consoles with network connections to
3 facilitate connection to a local area network, the first and second
4 game consoles running a same game title and being configured to
5 generate identical keys by virtue of running the same game title; and

6 the first game console being configured to discover the
7 second game console by broadcasting messages over the local area
8 network, the messages being secured by the keys.

9 In making out a rejection of claim 52, the Office states that Rothschild
10 teaches most of the elements of the claim, including first and second game
11 consoles, that Perlman teaches an LAN network and that Chatani teaches
12 “generating identical keys.” (*Office Action of 7/12/05*, page 14).

13 For the reasons given above with respect to claims 6 and 13, the references
14 do not disclose this system. Namely, the cited reference does not disclose “first
15 and second game consoles,” as recited in Applicant’s claim 52.

16 Applicant therefore respectfully requests allowance of claim 33.

17 **Dependent claims 53-54** depend from claim 52 and are allowable by virtue
18 of this dependency. Moreover, these claims recite features that, when taken
19 together with those of claim 52, define systems not taught or suggested by
20 Rothschild, Perlman and Chatani.

21 Rothschild in view of Perlman in view of Nguyen

22 Claims 40-42 stand rejected under 35 U.S.C. § 103(a) as being unpatentable
23 over Rothschild in view of Perlman in further view of Nguyen. Applicant
24 respectfully traverses the rejection.
25

1 Nguyen describes a gaming machine that may securely communicate with
2 devices over a public network such as the internet. The gaming machine utilizes a
3 combination of symmetric and asymmetric encryption that allows a single gaming
4 machine to securely communicate with a remote server using a public network.
5 (*Nguyen*, abstract).

6 **Independent claim 40** recites a computer-readable medium for a game
7 console comprising computer-executable instructions that, when executed, direct
8 the game console to:

9 encrypt a request to join in playing a game title being hosted
10 by a remote host game console on a local area network;

11 digitally sign the request;
12 broadcast the request over the local area network;

13 listen for at least one broadcast reply from the host game
14 console;

15 upon receipt of the reply, extract at least one session key from
16 the reply for use in facilitating future communication with the host
17 game console;

18 form an initial packet that contains first data used to derive a
19 cryptographic key;

20 compute a first hash digest of the initial packet using the
21 session key;

22 send the initial packet and the first hash digest to the host
23 game console;

24 listen for a reply packet from the host game console, the reply
25 packet including a second hash digest and second data;

 authenticate the reply packet using the session key and the
 second hash digest; and

1 derive at least one security association key from the first and
2 second data, the security association keys being used to secure
3 communication with the host game console.

4 In making out a rejection of claim 40, the Office cites Rothschild for many
5 of the claims elements, but states that Rothschild does “not disclose digitally
6 signing the reply.” Nevertheless, the Office cites Nguyen as teaching such an
7 element. (*Office Action of 7/12/05*, page 16). Applicant respectfully traverses the
8 rejection.

9 For the reasons given above with respect to claims 6 and 13, the references
10 do not teach or suggest the claimed medium. Namely, the cited references do not
11 teach or suggest a computer-readable medium that “direct[s] the game console to
12 encrypt a request to join in playing a game title being hosted by a remote host
13 game console on a local area network,” as recited in Applicant’s claim 40. In fact,
14 the references do not teach multiple game consoles, as the server MCP in
15 Rothschild is not a game console.

16 Applicant therefore respectfully requests allowance of claim 40.

17 Furthermore, the cited references do not teach or suggest this claim for at
18 least the reasons given above with respect to claim 25. Namely, the references do
19 not teach “comput[ing] a first hash digest.” For at least this additional reason,
20 claim 40 is allowable.

21 **Independent claim 41** recites a computer-readable medium for a game
22 console comprising computer-executable instructions that, when executed, direct
23 the game console to:

24 receive a request from a remote game console on a local area
25 network, the request seeking network play of a game title;

1 authenticate the request as being generated by an authentic
2 game console running an authentic version of the game title;

3 decode the request;

4 determine whether to allow the remote game console to play;

5 in an event the remote game console is allowed to play, create
6 a reply with containing at least one session key;

7 encrypt and digitally sign the reply;

8 send the reply to the remote game console;
9 receive an initial packet directly from the remote game
10 console, the initial packet containing first data used to derive a
cryptographic key;

11 authenticate the initial packet using the session key;

12 form a response packet holding second data used to derive a
13 cryptographic key;

14 send the response packet to the remote game console; and

15 derive at least one security association key from the first and
16 second data, the security association keys being used to secure
communication with the remote game console.

17
18 In making out a rejection of claim 41, the Office cites Rothschild for many
19 of the claims elements, but states that Rothschild does “not disclose digitally
20 signing the reply.” Nevertheless, the Office cites Nguyen as teaching such an
21 element. (*Office Action of 7/12/05*, page 17). Applicant respectfully traverses the
22 rejection.
23
24
25

1 For the reasons given above with respect to claims 6 and 13, the references
2 do not teach or suggest the claimed medium. Namely, the cited references do not
3 teach or suggest a computer-readable medium that “direct[s] the game console to
4 receive a request from a remote game console,” as recited in Applicant’s claim 41.
5 In fact, the references do not teach multiple game consoles, as the server MCP in
6 Rothschild is not a game console.

7 Applicant therefore respectfully requests allowance of claim 40.

8 **Dependent claim 42** depends from claim 41 and is allowable by virtue of
9 this dependency. Moreover, this claim recites features that, when taken together
10 with those of claim 41, define a system not taught or suggested by Rothschild,
11 Perlman and Nguyen.

12
13 Rothschild in view of Perlman and Chatani in further view of Murphy

14 Claim 28 stands rejected under 35 U.S.C. § 103(a) as being unpatentable
15 over Rothschild in view of Perlman and Chatani in further view of Murphy.
16 Applicant respectfully traverses the rejection.

17 **Dependent claim 28** recites a “method as recited in claim 27, wherein the
18 deriving comprises computing a hashing function on a concatenation of the
19 console-based key and the title-based key.” In making out a rejection of claim 28,
20 the Office relies upon the earlier rejection of claim 27, discussed above. The
21 Office then further cites Murphy for teaching the additional element of claim 28.

22 As discussed above, however, Rothschild, Perlman, nor Chatani teach or
23 suggest independent claim 27. Namely, the cited references do not teach or
24 suggest “exchanging packets between the first and second game consoles,” nor
25 “establishing a secure communication link between the first and second game

1 consoles,” as a server MCP does not constitute a host game console. Furthermore,
2 Murphy is not cited for teaching such an element, nor does it teach such an
3 element, and therefore does not add anything of substance to the rejection.
4 Therefore, claim 28 is allowable for at least the reasons discussed above in regards
5 to claims 6 and 13.

6 Furthermore, the cited references do not teach “deriving at least one
7 cryptographic key from the console-based key and the title-based key,” as recited
8 by base claim 27. Therefore, claim 28 is additionally allowable for at least the
9 reasons discussed above in regards to claims 2 and 3.

10 Applicant therefore respectfully requests allowance of claim 28.

11
12 Rothschild in view of Perlman and Chatani in further view of Nguyen

13 Claim 29 stands rejected under 35 U.S.C. § 103(a) as being unpatentable
14 over Rothschild in view of Perlman and Chatani in further view of Nguyen.
15 Applicant respectfully traverses the rejection.

16 **Dependent claim 29** recites a “method as recited in claim 27, wherein the
17 deriving comprises computing an encryption key and a signature key; and the
18 encoding of the request comprises encrypting the request using the encryption key
19 to form an encrypted request and digitally signing the encrypted request using the
20 signature key.”

21 In making out a rejection of claim 29, the Office relies upon the earlier
22 rejection of claim 27, discussed above. The Office then further cites Nguyen for
23 teaching the additional element of claim 29.

24 As discussed above, however, Rothschild, Perlman, nor Chatani teach or
25 suggest independent claim 27. Namely, the cited references do not teach or

1 suggest "exchanging packets between the first and second game consoles," nor
2 "establishing a secure communication link between the first and second game
3 consoles," as a server MCP does not constitute a host game console. Furthermore,
4 Nguyen is not cited for teaching such an element, nor does it teach such an
5 element, and therefore does not add anything of substance to the rejection.
6 Therefore, claim 29 is allowable for at least the reasons discussed above in regards
7 to claims 6 and 13.

8 Furthermore, the cited references do not teach "deriving at least one
9 cryptographic key from the console-based key and the title-based key," as recited
10 by base claim 27. Therefore, claim 29 is additionally allowable for at least the
11 reasons discussed above in regards to claims 2 and 3.


12 Applicant therefore respectfully requests allowance of claim 29.

13
14 **Conclusion**

15 Claims 1-54 are in condition for allowance. Applicant respectfully requests
16 reconsideration and prompt allowance of the subject application. If any issue
17 remains unresolved that would prevent allowance of this case, the Examiner is
18 requested to contact the undersigned attorney to resolve the issue.

19
20
21 Date: Oct. 11, 2005

Respectfully Submitted,

22 By: 
23 Lewis C. Lee
24 Lee & Hayes, pllc
25 Reg. No. 34,656
(509) 324-9256 ext. 211